UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS

KATRINA WALKER, on behalf of herself and all others similarly situated, Plaintiffs v. NATIONSTAR FINANCIAL, INC., d/b/a MR. COOPER, Defendant	Civil Action No.: 3:23-cv-2524 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Katrina Walker ("Walker" or "Plaintiff"), by and through her attorneys of record, upon personal knowledge as to her own acts and experiences, and upon information and belief, which Plaintiff believes will be a supplemented and supported after a reasonable opportunity for discovery as to all other matters, brings this class action complaint against defendant Nationstar Financial, Inc., d/b/a Mr. Cooper ("Defendant" or "Mr. Cooper"), and alleges as follows:

INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard Plaintiff's and Class Members' protected "personally identifiable information" or "PII" (also referred to herein as "Private Information").[1]

[1] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

2. Defendant is the third largest mortgage servicer in the United States, servicing mortgages valued at approximately $937 billion on behalf of approximately 4.3 million customers throughout the United States.

3. In the course of servicing the mortgages of class members, Defendant acquired and collected Plaintiff's and Class Members' PII. Defendant knew, at all times material, that it was collecting, and responsible for the security of sensitive data, including Plaintiff's and Class Members' highly confidential PII. This PII remains in the possession of Defendant, despite the fact that it was accessed by unauthorized third persons and is currently being maintained without appropriate and necessary safeguards, independent review, and oversight, and therefore remains vulnerable to additional hackers and theft.

4. Plaintiff seeks to hold Defendant responsible for the harms it caused and will continue to cause Plaintiff and approximately 4.3 million other similarly situated persons by virtue of a massive and preventable cyberattack that began no later than October 31, 2023, by which cybercriminals infiltrated Defendant's computer network on which the Private Information that Defendant was entrusted with and responsible for, was stored (the "Data Breach"). Plaintiff further seeks to hold Defendant responsible for not ensuring that the PII was maintained in a manner consistent with industry standards.

5. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Plaintiff's and Class Members' PII.

6. The Data Breach occurred because Defendant maintained Class Members' PII in a reckless manner and on its computer networks in a condition that was vulnerable to cyber-attacks. The risk of cyber-attack was well-known to Defendant – and to all mortgage and loan servicing

companies – and Defendant was continuously on notice at all times material that its failure to take steps necessary to secure the PII from a risk of cyber-attack and unauthorized access left that information and property in a dangerous condition that was vulnerable to theft.

7. Defendant knew or should have known of the cyber-attack by no later than October 31, 2023. Nonetheless, as of the date of filing of this complaint, Defendant has not notified victims of the data breach. Indeed, Plaintiff and Class Members do not, as yet, know what PII of theirs was accessed in the Data Breach, nor would Class Members know that the Data Breach impacted the Personal Information of consumers absent reading about it in the news or visiting Defendant's website. Indeed, even on Defendant's website, disclosure of the fact that the PII of Class Members was accessed in the Data Breach is buried on a subpage.

8. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties to those individuals. These duties arise from state and federal statutes and regulations, as well as common law principles.

9. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, upon information and belief, the PII of Plaintiff and Class Members was compromised and damaged through access by and disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Plaintiff and Class Members in the future – and are entitled to damages. In addition,

Plaintiff and Class Members, who have a continuing interest in ensuring that their information is and remains safe, are entitled to injunctive and other equitable relief.

PARTIES

Plaintiff Katrina Walker

10. Plaintiff Katrina Walker is, and at all relevant times was, a citizen of the state of Illinois and a resident of Chicago. Plaintiff Walker's home mortgage was transferred from Rushmore Loan Management to Defendant approximately three months ago. Prior to said transfer, Rushmore Loan Management had serviced Plaintiff Walker's loan since approximately 2017. In applying for her home mortgage, Plaintiff Walker provided substantial Personal Information, including, but not limited to, her full name, contact information, Social Security Number, birthdate, driver's license number, and financial account information. On information and belief, all of this critical PII was transferred to Defendant when it took over the servicing of her mortgage loan.

11. Plaintiff Walker takes care in protecting her PII from disclosure. Faced with the risk of the unauthorized disclosure of her PII, Plaintiff Walker is no forced to monitor her financial accounts for signs of fraud and identity theft.

Defendant Nationstar Financial, Inc., d/b/a Mr. Cooper

12. Mr. Cooper is the third largest mortgage servicer in the United States, servicing mortgages valued at approximately $937 billion on behalf of approximately 4.3 million customers. Nationstar was founded in 1994 as Nova Credit Corporation. Thereafter, it became the in-house lending arm of home builder Centex Homes, doing business as Centex Credit Corporation and thereafter changing it's name to Nationstar. In August 2017, Nationstar began doing business under the name Mr. Cooper in an effort to "personalize the mortgage experience." The Company maintains its headquarters at 8950 Cypress Waters Blvd., Coppell, Texas, a suburb of Dallas. Mr.

Cooper describes itself as being "led by a team of proven innovators and visionaries. Combining decades of experience in the mortgage industry with tenures in fields like tech, finance and real estate, these leaders have come together to transform the way people buy, sell and own their homes."[2] Defendant further asserts that it is a "champion[] for our customers," "always having your back," and "on your team."[3]

13. Defendant acquired, utilized, and stored the PII of the Plaintiff named herein and Class Members respecting whom Plaintiff seeks to represent.

JURISDICTION AND VENUE

14. This Court has original jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2), because the matter in controversy, exclusive of interest and costs, exceeds the sum value of $5,000,000.00, consists of putative class membership of greater than 100 members, and is a class action in which some of the members of the Class, are citizens of states different than that of Defendant.

15. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because Defendant is authorized to conduct business within this District, is headquartered in this District, has intentionally availed itself of the laws in this District, and conducts substantial business, including acts underlying the allegations of this complaint, in this District.

FACTUAL BACKGROUND

The Data Breach

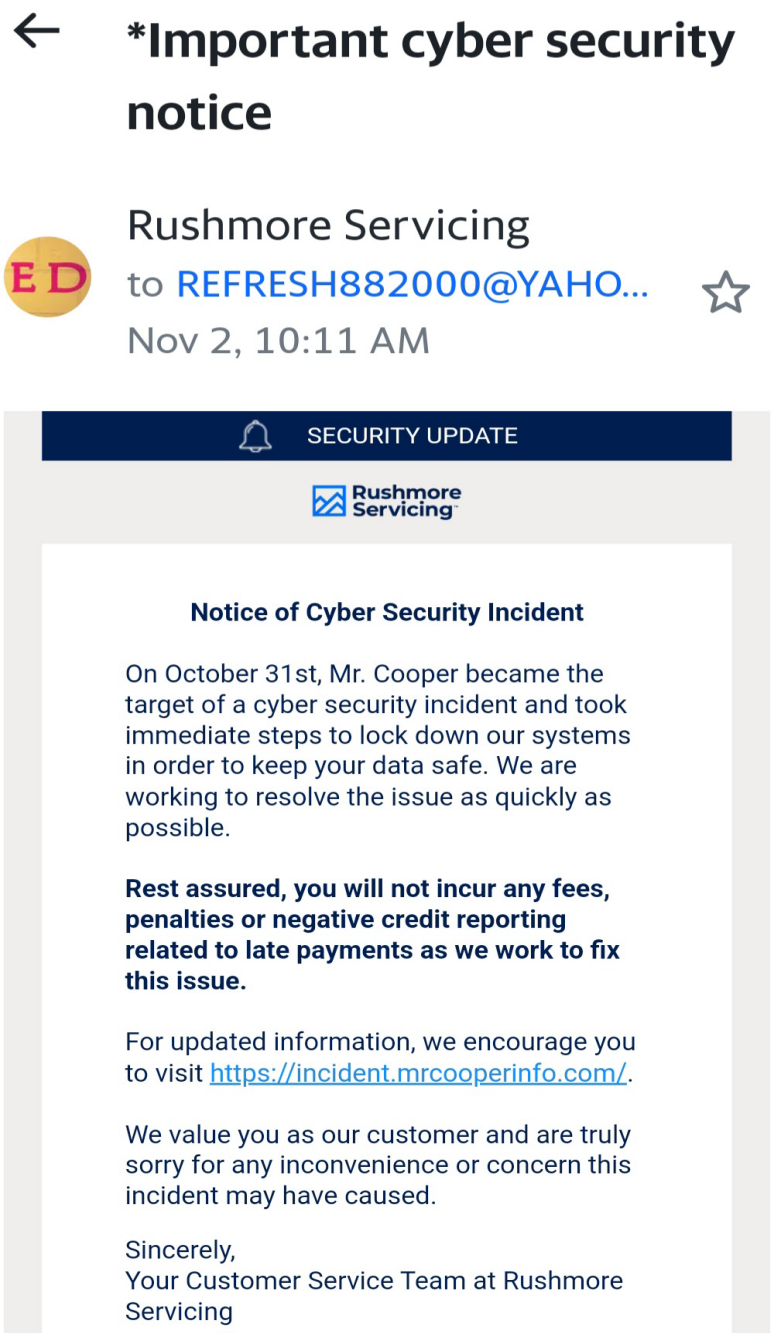
16. On or about November 2, 2023, Defendant announced that its computer network had been "the target of a cybersecurity incident" and that it had taken "immediate steps to lock

[2] https://www.mrcooper.com/about-us/leadership last visited on November 9, 2023.

[3] https://www.mrcooper.com/about-us/purpose last visited on November 9, 2023.

down our systems in order to keep your data safe."[4] Initially, the company asserted that the breach was limited to Mr. Cooper's internal systems and that customer data had not been accessed. *Id.* Mr. Cooper spokesperson Sarah Rutledge claimed that "we believe this cybersecurity incident was isolated to Mr. Cooper systems and technology and did not affect any of the company's clients' or partners' systems or technology." *Id.* This was not true and, in the days following the cyberattack, customers of Mr. Cooper, like Plaintiff, were left with a false sense of confidence that their PII was safe. Even in direct communications with Class Members informing them of a "cyber security incident," Defendant failed to warn Class Members that their data had been compromised. A November 2, 2023 email to Plaintiff Walker repeated the Company's assertion that it had taking "immediate steps to lock down our systems in order to keep your data safe[,]" without disclosing the breach of customer data.

[4] https://nationalmortgageprofessional.com/news/mr-cooper-locked-down-cyber-attack last visited November 9, 2023.



*Important cyber security notice

Rushmore Servicing
to REFRESH882000@YAHO...
Nov 2, 10:11 AM

SECURITY UPDATE

Rushmore Servicing

Notice of Cyber Security Incident

On October 31st, Mr. Cooper became the target of a cyber security incident and took immediate steps to lock down our systems in order to keep your data safe. We are working to resolve the issue as quickly as possible.

Rest assured, you will not incur any fees, penalties or negative credit reporting related to late payments as we work to fix this issue.

For updated information, we encourage you to visit https://incident.mrcooperinfo.com/.

We value you as our customer and are truly sorry for any inconvenience or concern this incident may have caused.

Sincerely,
Your Customer Service Team at Rushmore Servicing

17. Indeed, at least until November 7, 2023, the Company had not acknowledged that hackers had accessed the PII of Plaintiff and Class Members.

18. Meanwhile, customers suffered numerous other impacts including, but not limited to, being unable to access accounts, make payments, and confirm payments made, even while being left unaware that their PII was impacted by the Data Breach.

19. Eventually, Defendant was forced to back track, acknowledging that "certain customer data was exposed."[5] However, even this acknowledgement was buried. Despite acknowledging the Data Breach on its website, the Company failed to use its homepage to inform consumers and begin the process of notifying them the Data Breach had impacted customer PII. Instead, Defendant buried the information, referring to it only via a webpage linked at the bottom of a "System Update." *Id*.

> **System Update as of 11/9/23**: On October 31, 2023, Mr. Cooper experienced a cybersecurity incident. As of today, our phone systems and website have been partially restored. You can now make payments and access limited information about your loan. Please note, your online account may not reflect your latest activity, but we are working to get everything updated as soon as possible. For the latest information on how this affects our customers, please visit https://incident.mrcooperinfo.com.[6]

20. By November 9, 2023, but no sooner than November 7, Defendant finally acknowledged that the Data Breach impacted customer PII, stating in its "Notice of Cybersecurity Incident," that:

> As part of our ongoing investigation, we now believe that certain customer data was exposed. We are continuing to investigate precisely what information was exposed. In the coming weeks, we will mail notices to any affected customer and provide them with complimentary credit monitoring services.

21. Defendant, while not yet providing any remediation, or detailed notice to consumers, stated that:

---

[5] https://incident.mrcooperinfo.com/, last visited November 9, 2023.

[6] https://www.mrcooper.com, last visited on November 9, 2023.

> . . . it is always advisable to monitor your financial accounts and credit reports for any unauthorized activity. You should immediately report any unusual activity to your financial institution. You can also contact the three major credit bureaus to place a "fraud alert" on your file at no cost, which alerts creditors to contact you before they open a new credit account under your Social Security number. Additionally, you should update your passwords frequently and with increasing complexity, and be mindful to not use the same password across multiple personal accounts.

22. The statements made by Defendant amount to no real disclosure at all, as they fail to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

23. As of the filing of this complaint, Defendant has still failed to, *inter alia*, (a) provide details of the data accessed in the data breach; (b) provide notice to the impacted consumers; and (c) provide credit monitoring services to impacted consumers. With each day, indeed, each hour, that passes without these steps, Class Members face a heightened risk of identity theft and financial fraud.

24. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, ultimately causing the exposure of Private Information.

25. Upon information and belief, Defendant continues to maintain Plaintiff's PII, as well as that of all other Class Members.

Mr. Cooper's Business and Obligation to Preserve and Protect Confidentiality and Privacy

26. Defendant is a mortgage servicer, entrusted with highly sensitive PII, including names, contact information, financial account information, Social Security Numbers, credit information, and other highly sensitive PII.

27. Plaintiff and Class Members are current or former clients of Defendant who obtained service(s) through Defendant.

28. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

29. In its Privacy Policy (the "Privacy Policy") Defendant acknowledged that "[k]eeping financial information is one of our most important responsibilities."[7] Defendant assured consumers that "[o]nly those persons who need it to perform their job responsibilities are authorized to access your information. We take commercially reasonable precautions to protect your information and limit disclosure by maintaining physical, electronic and procedural safeguards."[8]

30. Plaintiff and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members, who value the confidentiality of their Private Information and demand security to safeguard their Private Information, took reasonable steps to maintain the confidentiality of their PII.

31. At all times material, Defendant was under a duty to adopt and implement reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties. And to that end, Defendant also has a legal duty created by

[7] https://www.mrcooper.com/privacy last visited November 9, 2023.

[8] *Id.*

contract, industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

32. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' Private Information. In addition, obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

33. Plaintiff is informed and believes and thereupon alleges that in order to obtain services from Defendant, Plaintiff and Class Members were required to provide PII and financial information, including the Private Information compromised in the Data Breach.

34. By obtaining, collecting, using, Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties, and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

35. Given the highly sensitive nature of the PII it possessed and the sensitivity of the services it provides, Defendant had a duty to safeguard, protect, and encrypt Plaintiff's and Class Members' PII.

36. Defendant retains and stores this information and derives a substantial economic benefit from the Private Information that it collects. But for the collection of Plaintiff's and Class Members' Private Information, Defendant would be unable to perform its mortgage servicing.

37. By obtaining, collecting, storing, and transmitting the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure.

38. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

39. Upon information and belief, Defendant made promises to Plaintiff and Class Members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

40. Defendant's negligence in safeguarding the Private Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

41. Defendant was not permitted to disclose Plaintiff's and Class Members' Private Information for any reason that would apply in this situation. The disclosure of Plaintiff's and Class Members' Private Information via the Data Breach was not permitted per Defendant's own privacy notice.

42. Defendant had obligations created by contract, industry standards, common law, and its own promises and representations made to Plaintiff and Class Members to keep their Private Information confidential and protect it from unauthorized access and disclosure.

43. Plaintiff and Class Members had a reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep the Private Information they provided confidential and secure from unauthorized access and disclosure.

44. Defendant failed to use reasonable security procedures and practices appropriate to safeguard the sensitive, unencrypted information it was maintaining for Plaintiff and Class

Members, consequently enabling and causing the exposure of Private Information of approximately 4.3 million individuals.

45. Because of Defendant's negligence and misconduct in failing to keep their information confidential, the unencrypted Private Information of Plaintiffs and Class Members has been expropriated by Unauthorized individuals who can now access the PII of Plaintiffs and Class Members and use it as they please.

46. Plaintiffs and Class Members now face a real, present and substantially increased risk of fraud and identity theft and have lost the benefit of the bargain they made with Defendant when receiving services.

Data Breaches Lead to Identity Theft and Cognizable Injuries.

47. The PII of consumers, such as Plaintiffs and Class Members, is valuable and has been commoditized in recent years.

48. Defendant was also aware of the significant repercussions that would result from its failure to do protect Private Information and knew, or should have known, the importance of safeguarding the Private Information entrusted to it and of the foreseeable consequences if its data security were breached. Nonetheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

49. Identity theft associated with data breaches is particularly pernicious due to the fact that the information is made available, and has usefulness to identity thieves, for an extended period of time after it is stolen. As a result, victims suffer both immediate and long-lasting exposure and are susceptible to further injury over the passage of time.

50. As a direct and proximate result of Defendant's conduct, Plaintiffs and the other Class Members have been placed at an imminent, immediate, and continuing increased risk of

harm from fraud and identity theft. They must now be vigilant and continuously review their credit reports for suspected incidents of identity theft, educate themselves about security freezes, fraud alerts, and take steps to protect themselves against identity theft, which will extend indefinitely into the future.

51. Even absent any adverse use, consumers suffer injury from the simple fact that information associated with their financial accounts and identity has been stolen. When such sensitive information is stolen, accounts become less secure, and the information once used to sign up for bank accounts and other financial services is no longer as reliable as it had been before the theft. Thus, consumers must spend time and money to re-secure their financial position and rebuild the good standing they once had in the financial community.

52. Plaintiffs and the other Class Members also suffer ascertainable losses in the form of opportunity costs and the time and costs reasonably incurred to remedy or mitigate the effects of the Data Breach, including:

A. Monitoring compromised accounts for fraudulent charges;

B. Canceling and reissuing credit and debit cards linked to the financial information in possession of Defendant;

C. Purchasing credit monitoring and identity theft prevention;

D. Addressing their inability to withdraw funds linked to compromised accounts;

E. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

F. Taking trips to banks and waiting in line to verify their identities in order to restore access to the accounts;

G. Placing freezes and alerts with credit reporting agencies;

H. Spending time on the phone with or at financial institutions to dispute fraudulent charges;

I. Contacting their financial institutions and closing or modifying financial accounts;

J. Resetting automatic billing and payment instructions from compromised credit and debit cards to new cards;

K. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised accounts that had to be cancelled; and,

L. Closely reviewing and monitoring financial accounts and credit reports for unauthorized activity for years to come.

53. Moreover, Plaintiffs and the other Class Members have an interest in ensuring that Defendant implement reasonable security measures and safeguards to maintain the integrity and confidentiality of the Private Information, including making sure that the storage of data or documents containing Private Information is not accessible by unauthorized persons, that access to such data is sufficiently protected, and that the Private Information remaining in the possession of Defendant is fully secure, remains secure, and is not subject to future theft.

54. As a further direct and proximate result of Defendant's actions and inactions, Plaintiffs and the other Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

55. As a direct and proximate result of Defendant's wrongful actions or omissions here, resulting in the Data Breach and the unauthorized release and disclosure of Plaintiff's and other

Class Members' Private Information, Plaintiffs and all Class Members have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including, *inter alia*, (i) the resulting increased and imminent risk of future ascertainable losses, economic damages and other actual injury and harm, (ii) the opportunity cost and value of lost time they must spend to monitor their financial accounts and other accounts—for which they are entitled to compensation; and (iii) emotional distress as a result of having their Private Information accessed and exfiltrated in the Data Breach.

Mr. Cooper Was Well Aware of the Threat of Cyber Theft and Exfiltration in the Financial and Mortgage Industries

56. As a condition of its relationships with its customers, Plaintiffs and Class Members, Defendant required that they entrust it with highly sensitive and confidential PII and financial information. Defendant, in turn, collected that information and assured consumers that it was acting to protect that PII and to prevent its disclosure.

57. Plaintiffs and Class Members were required to provide their Private Information with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access and disclosure.

58. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiffs and Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

59. Defendant could have prevented the Data Breach by assuring that the Private Information at issue was properly secured.

60. Defendant's overt negligence in safeguarding Plaintiff's and Class Members' PII is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years. Further, as an entity in the financial services space, Defendant was on notice that companies in that industry are targets for data breaches.

61. PII, including names and social security numbers are uniquely valuable to hackers. With these pieces of information, criminals can open new financial accounts in Class Member's names, take loans in their names, use their names to obtain medical services, obtain government benefits, file fraudulent tax returns in order to get refunds to which they are not even entitled, and numerous other assorted acts of thievery and fraud.

62. Social Security numbers are among the most sensitive kind of personal information. They are difficult for an individual to change. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against potential misuse of a Social Security number is not permitted; an individual instead must show evidence of actual, ongoing fraud to obtain a new number.[9]

63. A new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[10]

---

[9] Bryan Naylor, Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR (Feb. 9, 2015), available at: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions worrying-about-identity-theft (last accessed August 10, 2022)

[10] *Id.*

64. For this reason, hackers prey on companies that collect and maintain sensitive financial information, including financial institutions, mortgage servicers, and related entities. Companies like Defendant have been aware of this, and the need to take adequate measures to secure their systems and information, for a number of years. In 2021 alone, approximately 279 breaches targeting financial service providers occurred.[11] That figure represented a substantial increase from the year before and the year before that.[12] The steady growth of hacks of financial services providers is no surprise and can be tied to two significant factors, (1) the failure of financial services providers, like Defendant, to adequately protect patient data and (2) the substantial value of the sensitive PII entrusted to financial service providers.

65. In 2021, 1,862 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, an increase of 68% over 2020 and a 23% increase over the previous all-time high.[13] These data breaches exposed the sensitive data of approximately 294 million people. *Id.* Hackers are increasingly targeting highly sensitive PII, including social security numbers and, in 2021, approximately 1,136 data breaches exposed social security numbers. *Id.*

66. Companies like Mr. Cooper are well aware of the risk that data breaches pose to consumers, especially because both the size of their customer base and the fact that the PII that they collect and maintain is profoundly valuable to hackers. Indeed, Federal Reserve Chairman

---

[11] ITRC_2021_Data_Breach_Report.pdf (idtheftcenter.org) at 6. (last visited on August 10, 2022).

[12] *Id*.

[13] ITRC_2021_Data_Breach_Report.pdf (idtheftcenter.org) (last visited on August 10, 2022).

Jerome Powell has referred to cyber-attacks as the number one threat to the global financial system.[14]

67. It can be inferred from the Data Breach that Defendant either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Representative Plaintiff's and Class Members' PII.

68. Upon information and belief, prior to the Data Breach, Defendant was aware of its security failures but failed to correct them or to disclose them to the public, including Plaintiffs and Class Members.

69. The implementation of proper data security processes requires affirmative acts. Accordingly, Defendant knew or should have known that it did not make such actions and failed to implement adequate data security practices.

70. Because Defendant has failed to comply with industry standards, while monetary relief may cure some of Plaintiff's and Class Members' injuries, injunctive relief is necessary to ensure Defendant's approach to information security is adequate and appropriate. Defendant still maintains the PII of Plaintiffs and Class Members; and without the supervision of the Court via injunctive relief, Representative Plaintiff's and Class Members' PII remains at risk of subsequent data breaches.

71. In addition to its obligations under state and common laws, Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII and financial information in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant

---

[14] For Financial Institutions, Cyberthreats Loom Large (forbes.com) (last visited August 10, 2022).

owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII financial information of Plaintiffs and Class Members.

72. Defendant owed a duty to Plaintiffs and Class Members to ensure that the Private Information it collected and was responsible for was adequately secured and protected.

73. Defendant owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the PII and financial information in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

74. Defendant owed a duty to Plaintiffs and Class Members to implement processes that would immediately detect a breach that impacted the Private Information it collected and was responsible for in a timely manner.

75. Defendant owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

76. Defendant owed a duty to Plaintiffs and Class Members to disclose if its data security practices were inadequate to safeguard individuals' Private Information from theft because such an inadequacy would be a material fact in the decision to entrust this Private Information to Defendant.

77. Defendant owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

78. Defendant owed a duty to Plaintiffs and Class Members to mitigate the harm suffered by the Representative Plaintiff and Class Members as a result of the Data Breach.

Defendant Violated FTC Guidelines Prohibiting Unfair or Deceptive Acts

79. Mr. Cooper is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See e.g., FTC v. Wyndham Corp.*, 799 F.3d 236 (3d Cir. 2015).

80. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[15]

81. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[16]

82. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

83. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and

[15] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited November 8, 2023).

[16] https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited November 9, 2023).

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

84. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

85. Defendant was at all times fully aware of its obligations to protect Plaintiff's and Class Members' Private Information because of its business model of collecting Private Information and storing such information. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Value of the Relevant Sensitive Information

86. The high value of PII and financial information to criminals is evidenced by the prices they garner on the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[17] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[18] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[19]

87. These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members. For example, it is believed that certain PII compromised in

[17] Your personal data is for sale on the dark web. Here's how much it costs, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-darkweb-how-much-it-costs/ (last accessed November 9, 2023).

[18] *Id*.

[19] In the Dark, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed November 9, 2023).

the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Plaintiff and Class Members for the rest of their lives. They will need to remain constantly vigilant.

88. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

89. Identity thieves can use PII and financial information, such as that of Plaintiff and Class Members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

90. The ramifications of Defendant's failure to keep secure Plaintiff's and Class Members' PII are long lasting and severe. Once PII and financial information is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, the PII of Plaintiff and Class Members was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

91. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[20]

92. Data breaches are preventable.[21] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[22] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised."[23]

93. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[24]

---

[20] 47 Report to Congressional Requesters, GAO, at 29 (June 2007), available at: http://www.gao.gov/new.items/d07737.pdf (last accessed November 9, 2023).

[21] Lucy L. Thompson, Despite the Alarming Trends, Data Breaches Are Preventable, in DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)

[22] *Id*. at 17.

[23] *Id*. at 28.

[24] *Id.*

Defendant's Delayed Response to the Breach

94. Time is of the essence when highly sensitive PII is subject to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired PII of Plaintiff and Class Members is likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their PII, especially their Social Security numbers, onto the Dark Web. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing hundreds of thousands of Medicare numbers, Social Security numbers, Dates of birth, and other critical PII.

95. Despite this understanding, Defendant has not informed affected individuals, including Plaintiff and Class Members, about the Data Breach beyond statements to the press and postings on its website. Nor has it provided credit monitoring to affected consumers.

96. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.6% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[25]

97. According to the U.S. Bureau of Labor Statistics' 2022 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[26] leisure

[25] U.S. BUREAU OF LABOR STATISTICS, Wage Worker Survey, available at https://www.bls.gov/opub/reports/minimum-wage/2022/home.htm (last visited November 9, 2023); see also U.S. BUREAU OF LABOR STATISTICS, Employment And Average Hourly Earnings By Industry, available at https://www.bls.gov/news.release/empsit.t19.htm (last visited November 9, 2023) (finding that on average, private-sector workers make $1,166.20 per 40-hour work week).

[26] See https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html?&qsearchterm=James%20Wallman (last visited November 9, 2023).

time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[27] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

98. Plaintiff and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek remuneration for the loss of valuable time as another element of damages.

CLASS ALLEGATIONS

99. Pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), (b)(3), and (c)(4), Plaintiff asserts common law claims, as more fully alleged hereinafter, on behalf of the following Nationwide Class. In addition, Plaintiff asserts common law claims, as more fully alleged hereinafter, on behalf of an Illinois Class, defined as follows:

> **Nationwide Class**: All residents of the United States whose PII was accessed or otherwise compromised as a result of the Data Breach.
>
> **Illinois Class**: All residents of the state of Illinois whose PII was accessed or otherwise compromised as a result of the Data Breach.

Members of the Nationwide Class and the Illinois Class are referred to herein collectively as "Class Members" or "Class."

100. Excluded from the Class are Defendant, any entity in which Defendant have a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

---

[27] *Id.*

101. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

102. **Numerosity**: The exact number of members of the Class is unknown to Plaintiff at this time but Defendant provides services to millions of consumers throughout the United States.[28] Ultimately, members of the Class will be readily identified through Defendant's records.

103. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a) Whether Defendant failed to adequately safeguard Plaintiff's and the Class Members' PII;

b) Whether Defendant failed to protect Plaintiff's and the Class Members' PII, as promised;

c) Whether Defendant's computer system systems and data security practices used to protect Plaintiff's and the Class Members' PII violated federal, state, and local laws, or Defendant's duties;

d) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and the Class Members' PII properly and/or as promised;

e) Whether Defendant violated the consumer protection statutes, data breach notification statutes, state unfair practice statutes, state privacy statutes, and/or FTC law or regulations, imposing duties upon Defendant, applicable

[28] https://www.mrcooper.com last visited November 9, 2023.

to Plaintiff and Class Members;

f) Whether Defendant failed to notify Plaintiff and members of the Class about the Data Breach as soon as practical and without delay after the Data Breach was discovered;

g) Whether Defendant acted negligently in failing to safeguard Plaintiff's and the Class Members' PII;

h) Whether Defendant entered into contracts with Plaintiff and the Class Members that included contract terms requiring Defendant to protect the confidentiality of Plaintiff's PII and have reasonable security measures;

i) Whether Defendant's conduct described herein constitutes a breach of their contracts with Plaintiff and each of the Class Members;

j) Whether Defendant should retain the money paid by Plaintiff and each of the Class Members to protect their PII;

k) Whether Plaintiff and the Class Members are entitled to damages as a result of Defendant's wrongful conduct;

l) Whether Plaintiff and the Class Members are entitled to restitution as a result of Defendant's wrongful conduct;

m) What equitable relief is appropriate to redress Defendant's wrongful conduct; and

n) What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by Class Members.

104. **Typicality**: Plaintiff's claims are typical of the claims of each of the Class Members. Plaintiff and the Class Members sustained damages as a result of Defendant's uniform wrongful conduct during transactions with them.

105. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the Class, and have retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and there are no defenses unique to Plaintiff. Plaintiff and her counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Class, and have the financial resources to do so. Neither Plaintiff nor her counsel have any interest adverse to those of the other members of the Class.

106. **Separateness**: This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for the Defendant or would be dispositive of the interests of members of the proposed Class. Furthermore, the Private Information collected by Defendant still exists, and is still vulnerable to future attacks – one standard of conduct is needed to ensure the future safety of the PII of Plaintiff and Class Members.

107. **Class-wide Applicability**: This case is appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Plaintiff and proposed Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the Class, and making final injunctive relief appropriate with respect to the proposed Class as a whole. Defendant's practices challenged herein apply to and affect the members of the Class uniformly, and Plaintiff's challenge to those practices hinges on Defendant's conduct with respect to the proposed Class as a whole, not on individual facts or law applicable only to Plaintiff.

108. **Superiority**: This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and the members of the Class. The injuries suffered by each individual member of the Class are relatively small in comparison to the burden and expense of individual prosecution of the litigation necessitated by Defendant's conduct. Absent a class action, it would be virtually impossible for individual members of the Class to obtain effective relief from Defendant. Even if Class Members could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the common legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class and Illinois Class)

109. Plaintiff, on behalf of herself and the Class, re-alleges and incorporates the above allegations by reference.

110. Plaintiff and Class Members were required to submit PII to Defendant, in order to obtain services.

111. Defendant knew, or should have known, of the risks and responsibilities inherent in collecting and storing the PII of Plaintiff and Class Members.

112. As described above, Defendant owed a duty of care to Plaintiff and Class Members whose PII had been entrusted to Defendant.

113. Defendant breached its duty to Plaintiff and Class Members by failing to secure the PII that Defendant collected from consumers from unauthorized disclosure to third parties.

114. Defendant acted with wanton disregard for the security of Plaintiff's and Class Members' PII.

115. A "special relationship" exists between Defendant and the Plaintiff and Class Members. Defendant entered into a "special relationship" with Plaintiff and Class Members because it collected and/or stored the PII of Plaintiff and the Class Members.

116. But for Defendant's wrongful and negligent breach of its duty owed to Plaintiff and the Class Members, Plaintiff and the Class Members would not have been injured.

117. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duty. Defendant knew or should have known it was failing to meet its duty, and that Defendant's breach of such duties would cause Plaintiff and Class Members to experience the foreseeable harms associated with the unauthorized exposure of their PII.

118. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Nationwide Class and Illinois Class)

119. Plaintiff, on behalf of herself and the Class, re-alleges and incorporates the above allegations by reference.

120. Pursuant to the FTC Act (15 U.S.C. § 45, *et seq.*), Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' PII.

121. Defendant breached its duty to Plaintiff and Class Members by failing to implement reasonable safeguards to protect Plaintiff's and Class Members' PII from unauthorized access.

122. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

123. But for Defendant's wrongful and negligent breach of its duty owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

124. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duty, and that Defendant's breach of that duty would cause Plaintiff and Class Members to experience the foreseeable harms associated with the unauthorized access to their PII.

125. On information and belief, as a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III
Breach of Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiff and the Nationwide Class and Illinois Class)

126. Plaintiff, on behalf of herself and the Class, re-alleges and incorporates the above allegations by reference.

127. Plaintiff and Class Members entered into valid, binding, and enforceable express or implied contracts with entities affiliated with or serviced by Defendant, as alleged above.

128. The contracts respecting which Plaintiff and Class Members were intended beneficiaries were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations (both explicit

and fairly implied) and not to impair the rights of the other parties to receive the rights, benefits, and reasonable expectations under the contracts. These included the implied covenants that Defendant would act fairly and in good faith in carrying out its contractual obligations to take reasonable measures to protect Plaintiff's PII from unauthorized disclosure and to comply with state laws and regulations.

129. A "special relationship" exists between Defendant and the Plaintiff and Class Members. Defendant entered into a "special relationship" with Plaintiff and Class Members who sought services or treatment from Defendant and, in doing so, entrusted Defendant, pursuant to its requirements and Privacy Notice, with their PII.

130. Despite this special relationship with Plaintiff, Defendant did not act in good faith and with fair dealing to protect Plaintiff's and Class Members' PII.

131. Plaintiff and Class Members performed all conditions, covenants, obligations, and promises owed to Defendant.

132. Defendant's failure to act in good faith in complying with the contracts denied Plaintiff and Class Members the full benefit of their bargain, and instead they received services that were less valuable than what they paid for and less valuable than their reasonable expectations.

133. Accordingly, on information and belief, Plaintiff and Class Members have been injured as a result of Defendant's breach of the covenant of good faith and fair dealing respecting which they are express or implied beneficiaries, and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT IV
Breach of Duty
(On Behalf of Plaintiff and the Nationwide Class and Illinois Class)

134. Plaintiff, on behalf of herself and the Class, re-alleges and incorporates the above allegations by reference.

135. Defendant accepted the special confidence placed in it by Plaintiff and Class Members. There was an understanding between the parties that Defendant would act for the benefit of Plaintiff and Class Members in preserving the confidentiality of their PII.

136. Defendant became the guardian of Plaintiff's and Class Members' PII and accepted a fiduciary duty to act primarily for the benefit of its patients, including Plaintiff and the Class Members, including safeguarding Plaintiff's and the Class Members' PII.

137. Defendant breached its fiduciary duty to Plaintiff and Class Members by (a) failing to protect the PII of Plaintiff and the Class; (b) by failing to notify Plaintiff and the Class Members of the unauthorized disclosure of the PII; and (c) by otherwise failing to safeguard Plaintiff's and the Class Members' PII.

138. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and/or Class Members have suffered and/or will suffer injury, including but not limited to: (a) the compromise of their PII; and (b) the diminished value of the services they received as a result of unauthorized exposing of Plaintiff's and Class Members' PII.

139. On information and belief, as a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class and Illinois Class)

140. Plaintiff, on behalf of herself and the Class, re-alleges and incorporates by reference herein all of the allegations contained above.

141. Defendant collected and maintained responsibility for the Private Information of Plaintiff and the Class, including, *inter alia*, name, date of birth, address, Social Security Number, and other PII in connection with the provision of services to Plaintiff and the Class.

142. At the time Defendant acquired the PII of Plaintiff and the Class, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the PII and not take unjustified risks when storing the PII.

143. Plaintiff and the Class would not have entrusted their PII to Defendant had they known that Defendant would fail to adequately safeguard their PII.

144. Prior to the Data Breach, Defendant published the Privacy Notice, agreeing to protect and keep private financial information of Plaintiff and the Class.

145. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

146. In collecting and maintaining responsibility for the maintenance and protection of the PII of Plaintiff and the Class and publishing the Privacy Notice, Defendant entered into

contracts with Plaintiff and the Class requiring Defendant to protect and keep secure the PII of Plaintiff and the Class.

147. Plaintiff and the Class fully performed their obligations under the contracts with Defendant.

148. Defendant breached the contracts they made with Plaintiff and the Class by failing to protect and keep private financial information of Plaintiff and the Class.

149. On information and belief, as a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; additional time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, credit freezes, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

150. As a direct and proximate result of Defendant's breach of contract, Plaintiff and the Class are at an increased risk of identity theft or fraud.

151. As a direct and proximate result of Defendant's breach of contract, Plaintiff is entitled to and demand actual, consequential, and nominal damages and injunctive relief, to be determined at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of herself and the proposed Class, prays for relief and judgment against Defendant as follows:

A. certifying the Class pursuant to Rule 23 of the Federal Rules of Civil Procedure, appointing Plaintiff as representative of the Class, and designating Plaintiff's counsel as Class Counsel;

B. declaring that Defendant's conduct violates the laws referenced herein;

C. finding in favor of Plaintiff and the Class on all counts asserted herein;

D. awarding Plaintiff and the Class compensatory damages and actual damages, trebled, in an amount exceeding $5,000,000, to be determined by proof;

E. awarding Plaintiff and the Class appropriate relief, including actual, nominal and statutory damages;

F. awarding Plaintiff and the Class punitive damages;

G. awarding Plaintiff and the Class civil penalties;

H. granting Plaintiff and the Class declaratory and equitable relief, including restitution and disgorgement;

I. enjoining Defendant from continuing to engage in the wrongful acts and practices alleged herein;

J. awarding Plaintiff and the Class the costs of prosecuting this action, including expert witness fees;

K. awarding Plaintiff and the Class reasonable attorneys' fees and costs as allowable by law;

L. awarding pre-judgment and post-judgment interest; and

M. granting any other relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: November 14, 2023

Respectfully submitted,

STECKLER WAYNE & LOVE PLLC

By: */s/ Bruce W. Steckler*
BRUCE W. STECKLER
12720 Hillcrest Suite 1045
Dallas, Texas 75230
Telephone: (972) 387-4040
Facsimile: (972) 387-4041
bruce@swclaw.com

and

PAUL D. STICKNEY
Texas Bar No. 00789924
12720 Hillcrest Road, Suite 1045
Dallas, Texas 75230
Telephone: (972) 387-4040
Facsimile: (972) 387-4041
judgestick@gmail.com

BARRACK, RODOS & BACINE
STEPHEN R. BASSER*
SAMUEL M. WARD*
600 West Broadway, Suite 900
San Diego, CA 92101
Telephone: (619) 230-0800
Facsimile: (619) 230-1874
sbasser@barrack.com

EMERSON FIRM, PLLC
JOHN G. EMERSON
2500 Wilcrest, Suite 300
Houston, TX 77042
Phone: 800-551-8649
Fax: 501-286-4659

Counsel for Plaintiff Katrina Walker

**Pro Hac Vice* application to be filed